



Rec'd PCT/PT 10 SEP 2004

10/507291

15.09.03

BREVET D'INVENTION

REC'D 15 SEP 2003

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION PG:

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 13 AOUT 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

BEST AVAILABLE COPY



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

INPI
N° 11354*02

REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 9 W / 010801

REMISE DES PIÈCES DATE <u>07.06.02</u> LIEU <u>99</u> N° D'ENREGISTREMENT <u>0207168</u> NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE <u>07 JUIN 2002</u> PAR L'INPI		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE Patrice GUILLERM Schlumberger Systèmes BP 620-12 50 avenue Jean-Jaurès 92542 Montrouge cedex	
Vos références pour ce dossier (facultatif) 76.0731 FR			
Confirmation d'un dépôt par télécopie		<input checked="" type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
ou demande de certificat d'utilité initiale		N° _____ Date _____	
Transformation d'une demande de brevet européen		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Mise à jour d'un algorithme d'authentification dans un système informatique			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° EP n° 02075996.5 Date <u>11/03/2002</u> Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		SCHLUMBERGER SYSTEMES, S.A.	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN		<u>5621131530</u>	
Code APE-NAF		<u>50</u>	
Domicile ou siège		50 avenue Jean-Jaurès	
Rue			
Code postal et ville		<u>92120</u> Montrouge	
Pays		France	
Nationalité		Française	
N° de téléphone (facultatif)		<u>01 46 00 63 22</u> N° de télécopie (facultatif) <u>01 46 00 63 08</u>	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page

REMISE DES PIÈCES DATE 07.06.02 LIEU 99 N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0207168		Réservé à l'INPI	
Vos références pour ce dossier : (facultatif)		76.0731	
6 MANDATAIRE (s'il y a lieu)		[]	
Nom		GUILLERM	
Prénom		Patrice	
Cabinet ou Société		Schlumberger Systèmes	
N° de pouvoir permanent et/ou de lien contractuel		10219	
Adresse	Rue	50 avenue Jean-Jaurès BP 620-12	
	Code postal et ville	9 2 5 4 2 Montrouge cedex	
	Pays	France	
N° de téléphone (facultatif)		01 46 00 63 22	
N° de télécopie (facultatif)		01 46 00 63 08	
Adresse électronique (facultatif)		[]	
7 INVENTEUR (S)		Les inventeurs sont nécessairement des personnes physiques	
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> []	
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG [] [] [] [] []	
Si vous avez utilisé l'imprimé «Sulte», indiquez le nombre de pages jointes		[]	
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Patrice GUILLERM IP Engineer		VISA DE LA PRÉFECTURE OU DE L'INPI M MARTIN	

Mise à jour d'un algorithme d'authentification dans un système informatique.

Domaine technique

5 La présente invention se rapporte à la mise à jour d'un algorithme d'authentification dans un système informatique.

L'invention s'applique à tout dispositif de traitement de données stockant un algorithme d'authentification. L'invention s'applique tout particulièrement à la carte à puce.

10 La carte à puce peut être couplée avec tout système qu'il soit embarqué ou non.

L'invention peut être mise en œuvre dans tout type de réseau de télécommunication tel que le système de radiocommunication numérique cellulaire de type GSM (Global System for Mobile communication), UMTS (Universal Mobile Telecommunication Service), GPRS (General Packet Radio Service), etc.

L'exemple choisi pour illustrer l'invention sera celui du téléphone mobile couplé à une carte à puce de type SIM (Subscriber Identity Module).

20 Etat de la technique

La gestion de l'itinérance (roaming en anglais) d'un utilisateur dans un réseau GSM (Global System for Mobile Communication) nécessite la mise en œuvre d'une identification spécifique de cet utilisateur.

L'emploi d'un canal radio rend les communications vulnérables aux écoutes et aux utilisations frauduleuses. Le système GSM a donc recours

- à l'authentification de chaque utilisateur (ou abonné) avant de lui autoriser l'accès à un service,
- à l'utilisation d'une identité temporaire,
- au chiffrement (ou cryptage) des communications.

Le système GSM utilise actuellement quatre types de codes associés à l'abonné :

- 5 - Le code IMSI (International Mobile Subscriber Identity). Ce code est l'identité internationale d'un abonné. Cette identité est inscrite dans la carte SIM.
- Le code TMSI (Temporary Mobile subscriber Identity) est une identité temporaire attribuée par le réseau à un téléphone mobile et utilisé ensuite pour les transactions sur voie radio ;
- 10 - Le code MSISDN est le numéro international de l'abonné mobile conforme au plan E164 de l'UIT (Union Internationale des Télécommunications) et connu de l'abonné ;
- Le code MSRN (Mobile Station Roaming Number) est un numéro attribué temporairement, permettant par un appel téléphonique ordinaire de réaliser l'acheminement vers un commutateur MSC où
15 se trouve l'abonné mobile demandé.

Lors de l'abonnement, une clé Ki est attribuée à l'abonné avec le code IMSI. Ce couple IMSI/Ki est stocké à la fois dans la carte SIM de l'abonné et à l'extérieur de la carte notamment dans un centre d'authentification AuC
20 (Authentication Center en anglais). Un couple est intimement lié à un ou plusieurs algorithmes d'authentification.

Rappelons que le centre d'authentification AuC est un centre d'authentification des abonnés d'un réseau GSM. Rappelons, à titre
25 d'information, qu'une authentification est un processus permettant au réseau de vérifier qu'un abonné est autorisé à utiliser le réseau en contrôlant la présence d'une clé secrète dans la carte SIM.

Un autre couple peut également être stocké dans une seconde base de
30 données appelée HLR (Home Location Register). Cette base stocke le couple

MSISDN/IMSI associé à chaque abonné, constitué par le numéro de l'abonné MSISDN et l'identité invariante IMSI.

5 Un problème est celui de la mise à jour d'un algorithme stocké dans la carte, et dans tout dispositif de traitement de données stockant des données propres aux utilisateurs (le centre AuC, le registre HLR, la base VLR, etc.) communiquant avec la carte. Une telle mise à jour demande entre autres de modifier l'algorithme d'authentification de chaque couple IMSI/Ki, et des couples MSISDN/Ki, à la fois dans la carte et à l'extérieur de la carte dans le centre AuC,
10 dans le registre VLR, dans la base HLR, etc.

Une solution simpliste peut consister à télécharger le nouvel algorithme dans la carte et à l'extérieur de celle-ci dans le centre AuC, dans le registre VLR, dans la base HLR, etc. Cependant, cette solution pose problème en terme de
15 sécurité ; il n'est pas envisageable de transmettre cet algorithme sur le réseau, d'autant plus lorsque cet algorithme est non propriétaire.

L'invention

Un but visé est une mise à jour sécurisée d'un algorithme d'authentification.

20

En vue de la réalisation de ce but, l'invention se rapporte à un procédé de mise à jour d'un algorithme d'authentification dans au moins un dispositif de traitement de données apte à stocker dans une mémoire dudit dispositif une identité d'abonné associée à un algorithme d'authentification, caractérisé en ce
25 qu'il comprend les étapes suivantes :

- Une étape préalable de stockage, dans une mémoire du dispositif, d'un deuxième algorithme d'authentification inactif,
- Une étape de basculement du premier algorithme vers le deuxième algorithme (Algo2) propre à inhiber le premier algorithme et à activer
30 le second.

Ainsi, on voit que les algorithmes d'authentification sont stockés au préalable dans la carte. Ceci évite lors de la mise à jour de faire transiter un algorithme d'authentification pour une mise à jour.

- 5 L'invention sera mieux comprise à la lecture de la description qui suit, donnée à titre d'exemple et faite en référence aux dessins annexés.

Dans les dessins :

- 10 La figure 1 est une vue d'un système informatique sur lequel peut s'appliquer l'invention. Sur cette figure apparaît l'état de système informatique avant basculement des comptes.

La figure 2 représente la même vue que la figure 1. Sur cette figure, l'état du système est celui obtenu après basculement des comptes.

15 **Description détaillée illustrant l'invention.**

Pour simplifier la description, les mêmes éléments portent les mêmes références.

- 20 Sur la figure 1, de façon à illustrer l'invention, on a représenté une architecture comprenant un système embarqué tel qu'un téléphone mobile (non représenté) couplé à une carte CARD. Dans notre exemple de réalisation, cette carte est de type SIM.

Dans notre exemple illustré, le système embarqué communique avec un dispositif de traitement de données tel qu'un serveur SERV par l'intermédiaire d'un réseau de télécommunication RES.

- 25 Dans notre exemple, un opérateur OP gère les différentes cartes réparties sur le réseau. En particulier, l'opérateur gère les comptes des différents abonnés. En général, lors de la personnalisation de la carte, l'opérateur attribue un couple de données à savoir la clé Ki et le code IMSI associé à au moins un algorithme d'authentification et les charge dans la carte. La carte stocke ainsi un couple IMSI/Ki pour chaque abonné. Ce couple est également stocké dans un centre d'authentification AuC.
- 30

De façon à simplifier l'illustration de l'invention, on a choisi d'associer à chaque compte un unique algorithme d'authentification. Cependant, cet exemple n'est pas limitatif ; plusieurs algorithmes d'authentification auraient pu être associés à un même compte abonné.

5 Dans notre exemple illustré, un autre couple MSISDN/IMSI est stocké dans une base appelée HLR (Home Location Register).

Le centre AuC et la base HLR peuvent se trouver indifféremment sur un même serveur ou sur deux serveurs distincts. Dans notre exemple et en référence à la figure 1, on a choisi de les stocker sur le même serveur SERV.

10 Comme on l'a vu précédemment, une mise à jour d'un algorithme d'authentification n'est pas simple.

Dans notre exemple de réalisation, le procédé de mise à jour conforme à l'invention nécessite une carte à puce apte à stocker au moins deux comptes C1 et C2. La carte stocke un premier compte C1 d'abonné associé à au moins un premier algorithme d'authentification Algo1(A3A8). Ce premier compte est
15 constitué par le couple IMSI1/Ki1. Dans notre exemple illustré, la carte stocke également un deuxième compte C2 associé au même abonné A1 associé à au moins un second algorithme d'authentification Algo2(A3A8). Ce deuxième compte est constitué par le couple IMSI2/Ki2. L'invention ne se limite pas à
20 l'algorithme d'authentification A3A8 connu de l'homme du métier mais peut s'appliquer indifféremment à tout type d'algorithme d'authentification.

Dans la suite de la description, chaque compte C1 et C2 sera identifié par son code IMSI1 et IMSI2 respectif.

Dans notre exemple de réalisation, les comptes IMSI1 et IMSI2 sont gérés
25 par le même opérateur OP. Selon un autre mode de réalisation, les comptes sur la carte peuvent être gérés par des opérateurs différents.

De la même façon, dans notre exemple, le centre AuC stocke le compte IMSI1 associé au premier algorithme Algo1(A3A8) et le compte IMSI2 associé au deuxième algorithme Algo2(A3A8).

De la même façon, dans notre exemple, la base HLR stocke le couple MSISDN/IMSI1 associé au premier compte et le couple MSISDN/IMSI2 associé au deuxième compte.

Le procédé de mise à jour consiste à basculer le premier compte ISMI1 vers le deuxième ISMI2 dans la carte à puce, et le cas échéant dans le serveur SERV. Dans l'exemple de réalisation, le serveur SERV est équipé d'une fonctionnalité permettant de stocker deux comptes par abonné.

Pour cela, avant le basculement, le compte ISMI1 est actif, alors que le compte ISMI2 est inactif. La figure 1 est une vue du système avant le basculement des comptes. La figure 2 est une vue du système après le basculement.

Dans notre exemple de réalisation, les étapes de basculement des comptes sont les suivantes :

Etape 1

L'opérateur lance une commande propre à effectuer un basculement de compte. Avantageusement cette commande est une commande OTA (Over The Air) propre à activer un drapeau sur la carte, l'activation ayant un effet de basculement d'un compte vers un autre compte.

Un drapeau peut tout simplement être mis en œuvre par l'intermédiaire d'un bit. Par exemple, un bit à l'état 0 signifie que le compte ISMI1 est inactif et que le compte ISMI2 est actif. A l'inverse, un bit à l'état 1 signifie que le compte ISMI1 est actif et que le compte ISMI2 est inactif.

Etape 2

La carte CARD reçoit la commande et effectue un basculement de compte, du compte IMSI1 vers le compte IMSI2. A cet instant, dans la carte, le premier compte IMSI1 bascule de l'état actif vers l'état inactif IMSI2 et le second compte bascule de l'état inactif vers l'état actif.

Etape 3

Dans notre exemple, de façon à synchroniser le changement d'état des comptes stockés dans la carte avec ceux stockés dans le serveur SERV, le téléphone incluant la carte émet une commande d'authentification en direction du

serveur pour que celui-ci effectue un basculement des comptes. Cette commande d'authentification inclut le nouveau code IMSI2. Dans le serveur, le compte actif est le compte IMSI1. Lorsque le serveur reçoit la commande d'authentification, un programme est apte à identifier le nouveau code IMSI2. Le serveur SERV réalise alors un basculement d'algorithme de façon à assurer une synchronisation de la mise à jour des algorithmes d'authentification avec la carte CARD.

Dans le serveur, tous les couples (MSISDN/IMSI1 et IMSI1/Ki1) associés au premier algorithme Algo1(A3A8) deviennent inactifs, alors que tous les couples (MSISDN/IMSI2 et IMSI2/Ki2) associés au nouvel algorithme Algo2(A3A8) deviennent actifs. Tout comme sur la carte, le basculement peut être réalisé en activant un drapeau.

Etape 4

A ce stade du procédé, les deux comptes ISMI1 et ISMI2 ont basculé à la fois dans la carte CARD et dans le serveur SERV ; l'algorithme d'authentification utilisé pour l'authentification à la fois dans la carte CARD et dans le serveur SERV est désormais le nouvel algorithme Algo2(A3A8).

Les étapes décrites précédemment correspondent à un exemple de réalisation particulier non limitatif. L'étape 3 pourrait être mise en œuvre différemment :

- Par exemple, il n'est pas nécessaire de créer deux comptes ISMI1 et ISMI2. La carte peut stocker un unique compte et deux algorithmes d'authentification Algo1 et Algo2. L'opérateur peut tout simplement émettre simultanément une commande vers la carte et vers le serveur pour réaliser un basculement du premier algorithme Algo1 vers le deuxième algorithme Algo2 dans la carte et sur le serveur ;
Avantageusement, on peut prévoir des clés Ki différentes pour chaque algorithme Algo1 et Algo2.
- Ou, l'opérateur peut émettre une commande uniquement vers le serveur. Sur la carte, le compte actif est toujours le compte ISMI1.

Ultérieurement, lorsque le téléphone incluant la carte cherche à s'authentifier auprès du serveur SERV, celui-ci reçoit le code IMSI1 associé au premier algorithme Algo1 et s'aperçoit que le compte actuellement utilisé sur la carte n'est pas le compte ISMI2. Le serveur lance donc une commande propre à réaliser un basculement des comptes sur la carte. Une fois le basculement effectué, on peut prévoir que le téléphone incluant la carte émette vers le serveur un message informant que le basculement est bien effectué. A réception de ce message, les comptes basculent du compte ISMI1 vers le compte ISMI2 sur le serveur. Après basculement des comptes sur le serveur SERV, le serveur demande alors à la carte de s'authentifier avec le nouvel algorithme Algo2 associé au nouveau compte ISMI2.

- Ou, l'opérateur chargé du basculement peut télécharger dans la carte, et éventuellement dans le serveur, un programme apte à se déclencher à retardement par exemple en fonction d'une date définie et dont la fonction est de réaliser un basculement d'un compte vers un autre compte.

- Ou l'opérateur peut aussi déléguer l'opération de basculement à un ou plusieurs agents intelligents aptes à réaliser le basculement des comptes. Par exemple, on pourrait attribuer à chaque agent un ensemble de cartes. Dans cet exemple, l'opérateur transmet une commande à tout ou partie des agents pour qu'ils émettent en direction de la carte une commande COM ayant les mêmes caractéristiques que décrit précédemment.

- Le basculement des comptes sur le serveur peut être réalisé différemment. La carte s'authentifie auprès du serveur en utilisant le nouveau code IMSI2 associé au nouvel algorithme Algo2. Cependant l'algorithme Algo2 utilisé sur la carte n'est pas le même que l'algorithme actif sur le serveur SERV. En conséquence, l'authentification échoue ; cet échec peut servir de déclencheur au basculement des algorithmes sur le serveur.

Dans l'étape 3, le basculement peut ne pas être réalisé instantanément. Lorsque le drapeau est activé, on peut prévoir que le basculement effectif d'un compte vers un autre ne sera réalisé qu'après la réalisation d'un événement tel que la réinitialisation (Arrêt/Marche) de la carte, ou lors de l'exécution de la commande de rafraîchissement REFRESH en utilisant par exemple un mode parmi

- Reset,
- Full File Change Notification
- 10 - ou File Change Notification si la carte contient un fichier EF(IMSI) incluant le nouveau code IMSI.

Pour plus de détails sur ces modes, on se reportera aux textes des spécifications ETSI TS 11.14, TS 31.111 et TS 102 223 connus de l'homme du métier.

- 15 A noter que la mise à jour d'un algorithme d'authentification entraîne une modification des couples IMSI/Ki et MSISDN/IMSI. Une modification ne nécessite pas toujours de modifier les deux éléments constituant un couple. Une modification peut ne concerner qu'un seul élément. Par exemple, une modification d'un algorithme peut ne concerner que l'élément IMSI du couple
- 20 IMSI/Ki.

D'une manière générale, l'invention se rapporte à un procédé comprenant les étapes suivantes :

- Une étape préalable de stockage, dans une mémoire du dispositif, d'un deuxième algorithme d'authentification (Algo2) inactif,
- 25 - Une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2), propre à inhiber le premier algorithme (Algo1) et à activer le second (Algo2).

Avantageusement, l'étape de basculement est réalisée sur l'initiative d'une entité extérieure (OP) audit dispositif. Dans notre exemple de réalisation, cette

30 entité est un opérateur OP. Dans notre exemple, l'opérateur est maître de l'opération de basculement.

Dans notre exemple, l'opérateur qui émet la commande de basculement est un opérateur qui gère un compte actif sur la carte. Cependant, on peut prévoir qu'il existe des arrangements particuliers entre opérateurs s'autorisant mutuellement à effectuer des basculements de comptes sur la carte ; dans ce
5 contexte, on peut prévoir que l'opérateur qui émet la commande de basculement soit l'opérateur d'un compte inactif sur la carte. Plus généralement, l'étape de basculement est initiée, de préférence, par toute personne/entité autorisée à le faire.

De préférence, l'étape de stockage des algorithmes est réalisée dans un
10 endroit sûr, par exemple lors de la personnalisation de carte.

Le mode de basculement peut être mis en œuvre différemment. Par exemple, on a vu que l'opérateur chargé du basculement peut télécharger dans le dispositif un programme apte à se déclencher à retardement. Ainsi, le basculement peut être réalisé en même temps sur la carte, et sur tout dispositif
15 concerné par une mise à jour de l'algorithme d'authentification.

On a vu que la synchronisation de la mise à jour des algorithmes d'authentification sur la carte et le serveur peut être réalisée de différentes façons. Avantageusement, on stocke un deuxième compte C2 incluant un code IMSI2, différent du code IMSI1, associé à l'algorithme Algo2. Après l'étape de
20 basculement des comptes sur le dispositif en question, ce dernier transmet le code IMSI2 vers tout ou partie des dispositifs de traitement de données nécessitant un basculement d'algorithmes. Ce code IMSI2 a pour fonction notamment d'informer les dispositifs de traitement de données nécessitant un basculement d'algorithmes qu'un basculement a eu lieu. Ceci assure une
25 synchronisation de la mise à jour des algorithmes dans le système informatique. A réception du code (IMSI2) associé au deuxième algorithme (Algo2), ledit dispositif récepteur réalise un basculement d'algorithme du premier algorithme (Algo1) vers le second algorithme (Algo2).

La synchronisation peut être réalisée différemment. On a vu aussi dans
30 notre exemple, qu'après basculement, ledit dispositif peut transmettre tout

simplement une commande vers un autre dispositif de traitement de données nécessitant un basculement de comptes.

Avantageusement, à l'issue du basculement, l'espace mémoire stockant les données associées au compte désactivé est réutilisé. Par exemple, à l'issue du
5 basculement, les données associées au compte désactivé sont effacées de la mémoire. Cet effacement libère ainsi de l'espace mémoire.

On a vu aussi dans ce qui précède que, lors de la première étape, les deux comptes ISMI1 et ISMI2 créés dans la carte appartiennent au même abonné A1. A noter qu'un abonné peut rassembler un groupe d'utilisateurs utilisant le même
10 compte.

On a vu aussi, dans notre exemple de réalisation, que le basculement consiste à désactiver dans un premier temps le premier compte ISMI1 et à activer dans un second temps le second compte ISMI2.

15 Il en résulte un dispositif de traitement de données, en particulier une carte à puce, caractérisé en ce qu'il comprend :

- des moyens de mémoire stockant un deuxième algorithme d'authentification (Algo2),
- et en ce qu'il comprend un microcontrôleur programmé pour réaliser, sur
20 l'initiative d'un opérateur (OP), une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2).

L'invention concerne aussi un programme d'ordinateur pour un dispositif de traitement de données, comprenant des instructions de code pour l'exécution de
25 l'étape de basculement définie précédemment.

Enfin, l'invention concerne un programme d'ordinateur pour un dispositif de traitement de données, comprenant des instructions de codes pour, après l'étape de basculement du premier algorithme vers le second telle que définie dans la
30 revendication 1, identifier l'algorithme utilisé par un dispositif émetteur avec le

simplement une commande vers un autre dispositif de traitement de données nécessitant un basculement de comptes.

Avantageusement, à l'issue du basculement, l'espace mémoire stockant les données associées au compte désactivé est réutilisé. Par exemple, à l'issue du
5 basculement, les données associées au compte désactivé sont effacées de la mémoire. Cet effacement libère ainsi de l'espace mémoire.

On a vu aussi dans ce qui précède que, lors de la première étape, les deux comptes ISMI1 et ISMI2 créés dans la carte appartiennent au même abonné A1. A noter qu'un abonné peut rassembler un groupe d'utilisateurs utilisant le même
10 compte.

On a vu aussi, dans notre exemple de réalisation, que le basculement consiste à désactiver dans un premier temps le premier compte ISMI1 et à activer dans un second temps le second compte ISMI2.

15 Il en résulte un dispositif de traitement de données, en particulier une carte à puce, caractérisé en ce qu'il comprend :

- des moyens de mémoire stockant un deuxième algorithme d'authentification (Algo2),,
- et en ce qu'il comprend un microcontrôleur programmé pour réaliser, sur
20 l'initiative d'un opérateur (OP), une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2).

L'invention concerne aussi un programme d'ordinateur pour un dispositif de traitement de données, comprenant des instructions de code pour l'exécution de
25 l'étape de basculement définie précédemment.

Enfin, l'invention concerne un programme d'ordinateur pour un dispositif de traitement de données, comprenant des instructions de codes pour, après l'étape de basculement du premier algorithme vers le second, identifier l'algorithme
30 utilisé par un dispositif émetteur avec le code (IMSI2) reçu dudit dispositif émetteur.

code (IMSI2), tel que défini dans la revendication 5, reçu dudit dispositif émetteur.

On s'aperçoit que l'invention offre de nombreux avantages :

5 Le coût en temps d'une telle mise en œuvre est largement réduit. En effet, la carte est vendue avec les deux algorithmes. L'opérateur choisi lui-même le moment souhaité pour réaliser la migration. Une simple commande permet d'effectuer le basculement sur un nombre choisi de cartes à puce. L'opérateur a donc la possibilité s'il le souhaite de réaliser une migration à l'unité carte par
10 carte.

On a vu aussi qu'une fois le basculement effectué et que le nouvel algorithme Algo2 est actif, le compte associé à l'ancien algorithme Algo1 peut être effacé libérant ainsi de l'espace mémoire. Cette libération d'espace mémoire, en particulier dans la carte à puce, est un gros avantage vu les
15 contraintes matérielles extrêmes en terme de mémoire.

L'invention permet de ne pas remplacer toutes les cartes actuellement utilisées par de nouvelles cartes stockant la nouvelle version de l'algorithme d'authentification ;

L'invention permet d'éviter l'attribution d'un nouveau numéro de téléphone à
20 chaque abonné dont le couple IMSI/Ki nécessite d'être stocké dans un nouveau centre d'authentification AuC ; L'utilisateur conserve alors la même carte, le même numéro de téléphone dans tous les cas de figure.

L'invention permet à l'opérateur d'éviter des dépenses financières considérables. On voit que l'invention est intéressante pour l'opérateur car celui-ci utilise un seul centre d'authentification pour mettre à jour les algorithmes
25 d'authentification. L'opérateur n'est pas contraint d'acheter de nouveaux équipements pour effectuer la migration. Le coût en argent d'une telle mise en œuvre est encore une fois largement réduit.

On s'aperçoit que l'invention offre de nombreux avantages :

Le coût en temps d'une telle mise en œuvre est largement réduit. En effet, la carte est vendue avec les deux algorithmes. L'opérateur choisi lui-même le moment souhaité pour réaliser la migration. Une simple commande permet d'effectuer le basculement sur un nombre choisi de cartes à puce. L'opérateur a donc la possibilité s'il le souhaite de réaliser une migration à l'unité carte par carte.

On a vu aussi qu'une fois le basculement effectué et que le nouvel algorithme Algo2 est actif, le compte associé à l'ancien algorithme Algo1 peut être effacé libérant ainsi de l'espace mémoire. Cette libération d'espace mémoire, en particulier dans la carte à puce, est un gros avantage vu les contraintes matérielles extrêmes en terme de mémoire.

L'invention permet de ne pas remplacer toutes les cartes actuellement utilisées par de nouvelles cartes stockant la nouvelle version de l'algorithme d'authentification ;

L'invention permet d'éviter l'attribution d'un nouveau numéro de téléphone à chaque abonné dont le couple IMSI/Ki nécessite d'être stocké dans un nouveau centre d'authentification AuC ; L'utilisateur conserve alors la même carte, le même numéro de téléphone dans tous les cas de figure.

L'invention permet à l'opérateur d'éviter des dépenses financières considérables. On voit que l'invention est intéressante pour l'opérateur car celui-ci utilise un seul centre d'authentification pour mettre à jour les algorithmes d'authentification. L'opérateur n'est pas contraint d'acheter de nouveaux équipements pour effectuer la migration. Le coût en argent d'une telle mise en œuvre est encore une fois largement réduit.

Revendications

1. Procédé de mise à jour d'un algorithme d'authentification dans au moins un dispositif de traitement de données (CARD, SERV) apte à stocker dans une mémoire dudit dispositif (CARD, SERV) une identité d'abonné (IMSI1) associée à un algorithme d'authentification (Algo1), caractérisé en ce qu'il comprend les étapes suivantes :

- Une étape préalable de stockage, dans une mémoire du dispositif, d'un deuxième algorithme d'authentification (Algo2) inactif,
- 10 - Une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2) propre à inhiber le premier algorithme (Algo1) et à activer le second (Algo2).

2. Procédé selon la revendication 1, caractérisé en ce que l'étape de basculement est réalisée sur l'initiative d'une entité extérieure (OP) audit dispositif.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que, pour réaliser l'opération de basculement, l'entité extérieure audit dispositif (OP) transmet une commande (COM) à distance vers ledit dispositif (CARD) pour réaliser le basculement du premier algorithme (Algo1) vers le second algorithme (Algo2).

4. Procédé selon la revendication 1 ou 2, caractérisé en ce que pour réaliser l'opération de basculement, l'entité extérieure audit dispositif télécharge dans le dispositif un programme apte à se déclencher à retardement, et dont la fonction est de réaliser un basculement du premier algorithme (Algo1) vers le second algorithme (Algo2).

5. Procédé selon la revendication 1, caractérisé en ce que, lors de l'étape préalable de stockage, on stocke un deuxième code IMSI2, différent du code

Revendications

1. Procédé de mise à jour d'un algorithme d'authentification dans au moins un dispositif de traitement de données (CARD, SERV) apte à stocker dans une mémoire dudit dispositif (CARD, SERV) une identité d'abonné (IMSI1) associée à un algorithme d'authentification (Algo1), caractérisé en ce qu'il comprend les étapes suivantes :
 - Une étape préalable de stockage, dans une mémoire du dispositif, d'un deuxième algorithme d'authentification (Algo2) inactif,
 - Une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2) propre à inhiber le premier algorithme (Algo1) et à activer le second (Algo2).
2. Procédé selon la revendication 1, caractérisé en ce que l'étape de basculement est réalisée sur l'initiative d'une entité extérieure (OP) audit dispositif.
3. Procédé selon la revendication 1 ou 2, caractérisé en ce que, pour réaliser l'opération de basculement, l'entité extérieure audit dispositif (OP) transmet une commande (COM) à distance vers ledit dispositif (CARD) pour réaliser le basculement du premier algorithme (Algo1) vers le second algorithme (Algo2).
4. Procédé selon la revendication 1 ou 2, caractérisé en ce que pour réaliser l'opération de basculement, l'entité extérieure audit dispositif télécharge dans le dispositif un programme apte à se déclencher à retardement, et dont la fonction est de réaliser un basculement du premier algorithme (Algo1) vers le second algorithme (Algo2).
5. Procédé selon la revendication 1, caractérisé en ce que, lors de l'étape préalable de stockage, on stocke un deuxième code IMSI2, différent du code

IMSI1 et associé à l'algorithme Algo2, et en ce qu'après l'étape de basculement des comptes sur ledit dispositif (CARD), ledit dispositif transmet le code IMSI2 vers tout ou partie des dispositifs de traitement de données (SERV) nécessitant un basculement d'algorithmes, ledit code (IMSI2) associé au deuxième
 5 algorithme informant ces derniers du basculement d'algorithme de manière à assurer une synchronisation de la mise à jour des algorithmes.

6. Procédé selon la revendication 5, caractérisé en ce qu'à réception du code (IMSI2) associé au deuxième algorithme (Algo2), ledit dispositif récepteur
 10 réalise un basculement d'algorithme du premier algorithme (Algo1) vers le second algorithme (Algo2).

7. Procédé selon la revendication 1, caractérisé en ce qu'à l'issue du basculement, l'espace mémoire stockant les données associées au compte
 15 désactivé est réutilisé.

8. Dispositif de traitement de données, en particulier une carte à puce, apte à stocker une identité d'abonné (IMSI1) et associé à un algorithme d'authentification (Algo1), caractérisé en ce qu'il comprend :

20 - des moyens de mémoire stockant un deuxième algorithme d'authentification (Algo2),,

- et en ce qu'il comprend un microcontrôleur programmé pour réaliser, une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2) propre à inhiber le premier algorithme (Algo1) et à activer le
 25 second (Algo2).

9. Programme d'ordinateur pour un dispositif de traitement de données, comprenant des instructions de code pour l'exécution de l'étape de basculement définie dans la revendication 1.

30

IMS11 et associé à l'algorithme Algo2, et en ce qu'après l'étape de basculement des comptes sur ledit dispositif (CARD), ledit dispositif transmet le code IMSI2 vers tout ou partie des dispositifs de traitement de données (SERV) nécessitant un basculement d'algorithmes, ledit code (IMSI2) associé au deuxième
5 algorithme informant ces derniers du basculement d'algorithme de manière à assurer une synchronisation de la mise à jour des algorithmes.

6. Procédé selon la revendication 5, caractérisé en ce qu'à réception du code (IMSI2) associé au deuxième algorithme (Algo2), ledit dispositif récepteur
10 réalise un basculement d'algorithme du premier algorithme (Algo1) vers le second algorithme (Algo2).

7. Procédé selon la revendication 1, caractérisé en ce qu'à l'issue du basculement, l'espace mémoire stockant les données associées au compte
15 désactivé est réutilisé.

8. Dispositif de traitement de données, en particulier une carte à puce, apte à stocker une identité d'abonné (IMS11) et associé à un algorithme d'authentification (Algo1), caractérisé en ce qu'il comprend :
20 - des moyens de mémoire stockant un deuxième algorithme d'authentification (Algo2),,
- et en ce qu'il comprend un microcontrôleur programmé pour réaliser, une étape de basculement du premier algorithme (Algo1) vers le deuxième algorithme (Algo2) propre à inhiber le premier algorithme (Algo1) et à activer le
25 second (Algo2).

9. Programme d'ordinateur stocké dans un dispositif de traitement de données, comprenant des instructions de code pour l'exécution de l'étape de basculement définie dans la revendication 1 lorsqu'il est exécuté sur le dispositif
30 de traitement de données.

10. Programme d'ordinateur pour un dispositif de traitement de données, comprenant des instructions de codes pour, après l'étape de basculement du premier algorithme vers le second telle que définie dans la revendication 1, identifier l'algorithme utilisé par un dispositif émetteur avec le code (IMSI2), tel
- 5 que défini dans la revendication 5, reçu dudit dispositif émetteur.

10. Programme d'ordinateur stocké dans un dispositif de traitement de données, comprenant des instructions de codes pour, après l'étape de basculement du premier algorithme vers le second telle que définie dans la revendication 1, identifier l'algorithme utilisé par un dispositif émetteur avec le
5 code (IMSI2), tel que défini dans la revendication 5, reçu dudit dispositif émetteur lorsqu'il est exécuté sur le dispositif de traitement de données.

1/2

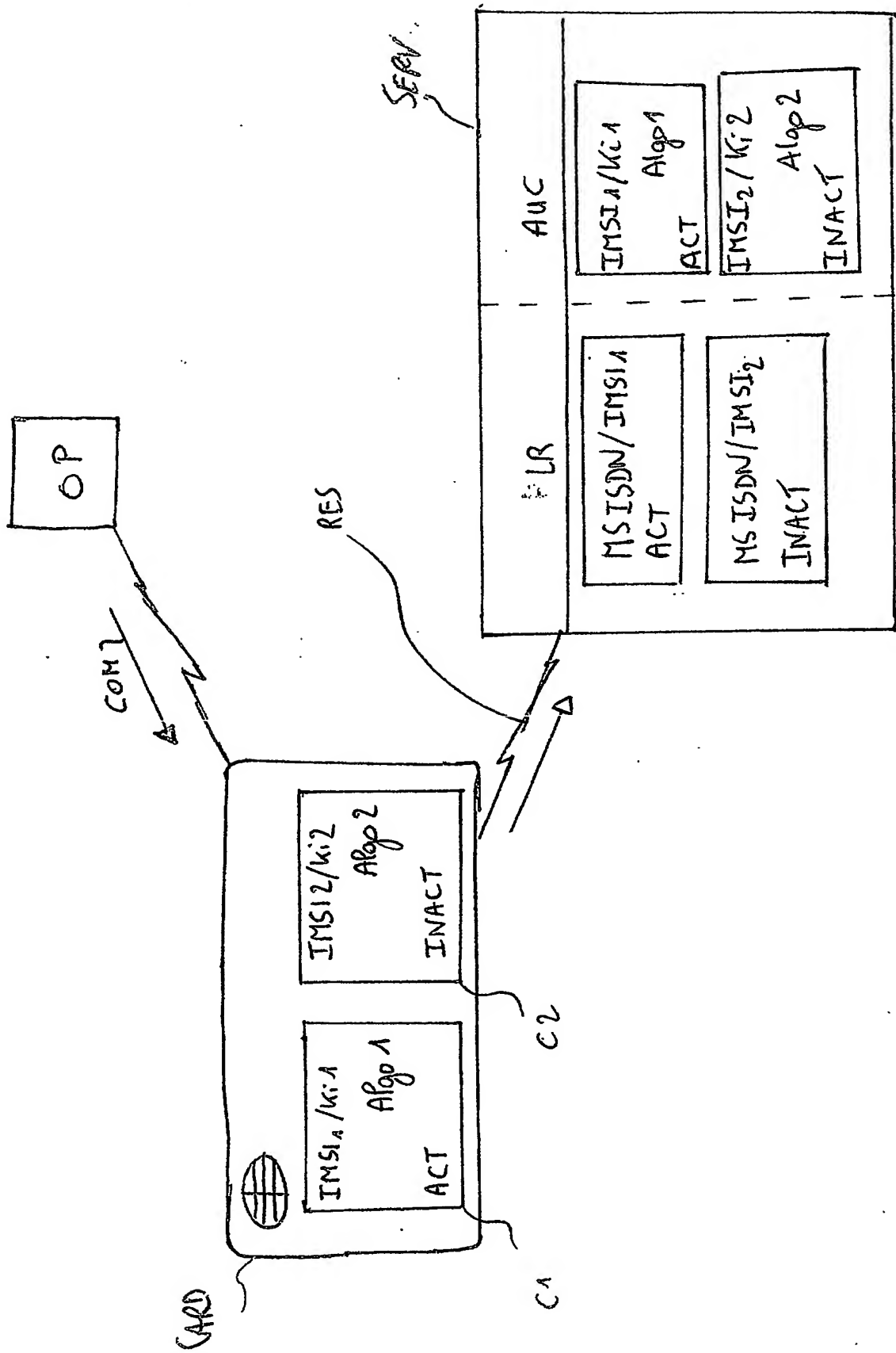
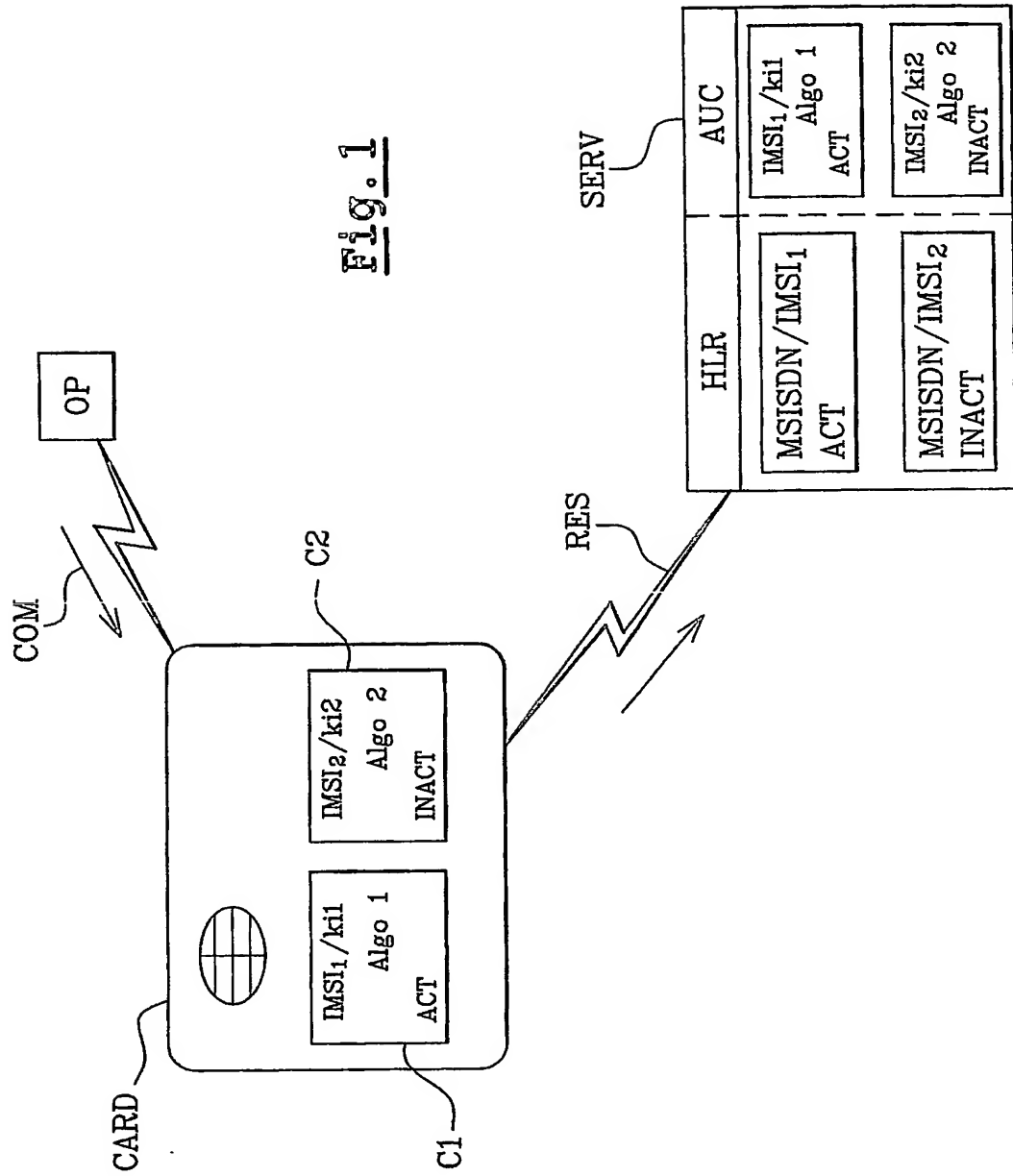


Figure 1



2/2

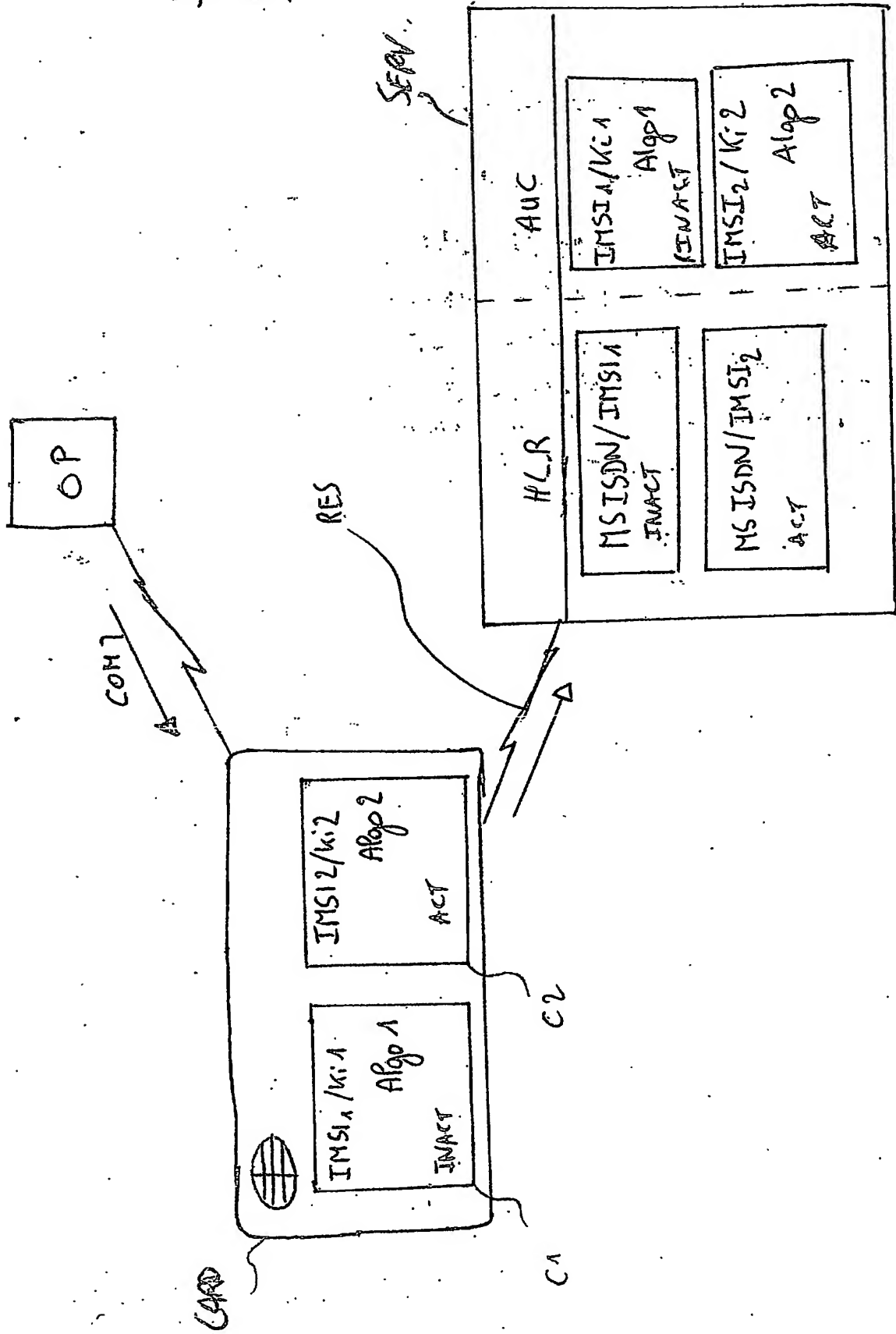
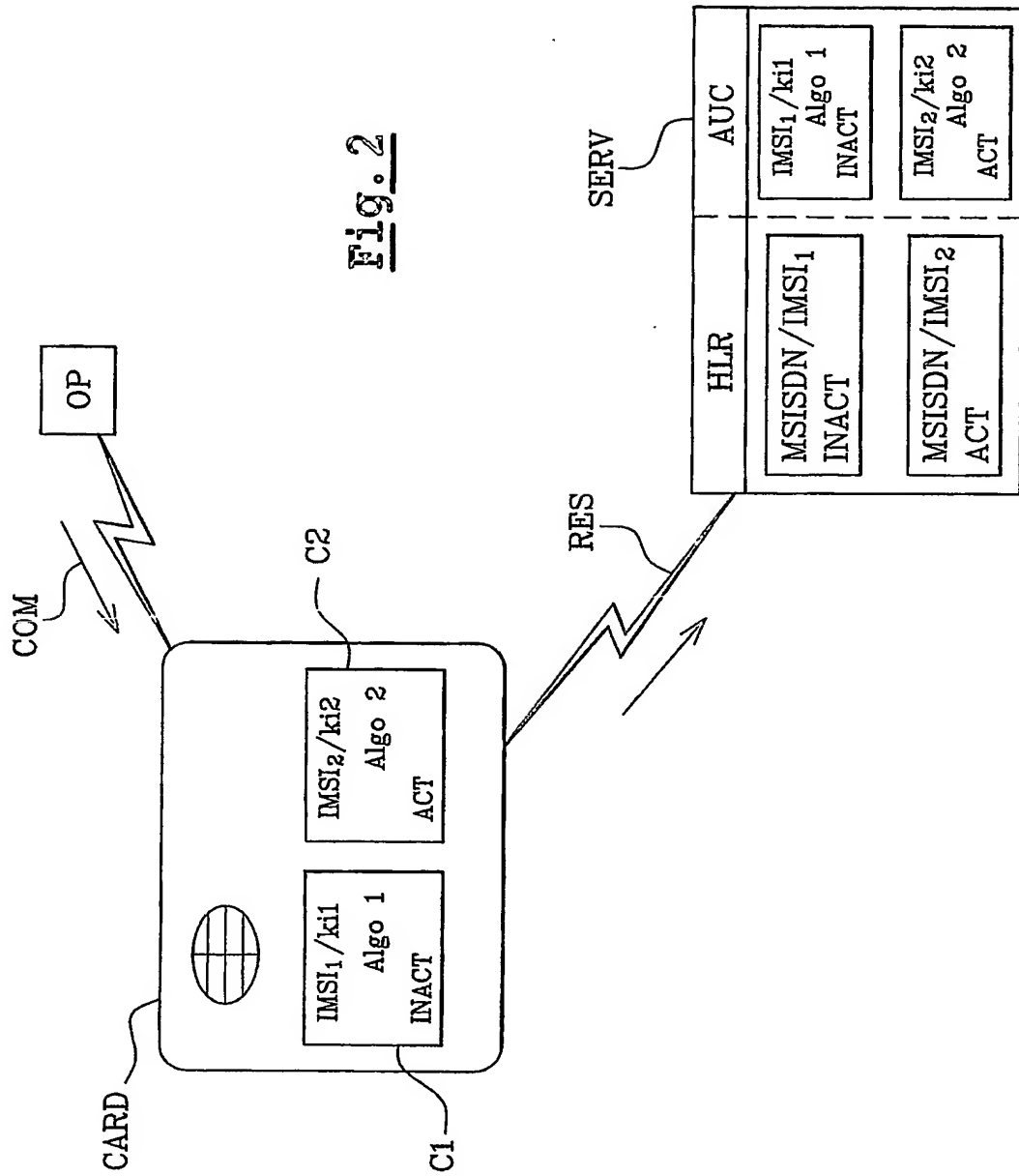


figure 2

Fig. 2

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

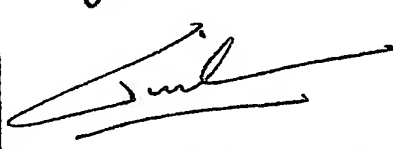
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		76.0731	
N° D'ENREGISTREMENT NATIONAL		0207168	
TITRE DE L'INVENTION (200 caractères ou espaces maximum) Mise à jour d'un algorithme d'authentification dans un système informatique			
LE(S) DEMANDEUR(S) : Schlumberger Systèmes 50 avenue Jean-Jaurès 92120 Montrouge France			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois Inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		BEAUDOU	
Prénoms		Patrice	
Adresse	Rue	27-29 rue Roque de Fillol	
	Code postal et ville	92800	Puteaux
Société d'appartenance (facultatif)			
Nom		DUBOIS	
Prénoms		Christophe	
Adresse	Rue	4 avenue Ursulines	
	Code postal et ville	78300	Poissy
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		7 juin 2002	
Patrice GUILLERM IP Engineer			

La loi n°78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.